

Galois Self-Dual Constacyclic Codes

Yun Fan and Liang Zhang

Dept of Mathematics, Central China Normal University, Wuhan 430079, China

Abstract

Generalizing Euclidean inner product and Hermitian inner product, we introduce Galois inner products, and study the Galois self-dual constacyclic codes in a very general setting by a uniform method. The conditions for existence of Galois self-dual and isometrically Galois self-dual constacyclic codes are obtained. As consequences, the results on self-dual, iso-dual and Hermitian self-dual constacyclic codes are derived.

Keywords: Constacyclic code, Galois inner product, q -coset function, isometry, Galois self-dual code.

MSC2010: 12E20, 94B60.

1 Introduction

Constacyclic codes over finite fields are a generalization of cyclic codes over finite fields, and inherit most of the advantages of cyclic codes. They can be theoretically studied with polynomials, and can be performed by feed-back shift registers in practice. There have been many references about the constacyclic codes. We are concerned with the research related to the duality and self-duality of constacyclic codes.

Let \mathbb{F}_q be a finite field with $q = p^e$ elements, where p is a prime. Let λ be a non-zero element of \mathbb{F} , and n be a positive integer. As usual, $\mathbb{F}_q[X]$ denotes the polynomial ring. Each element $\sum_{i=0}^{n-1} a_i X^i$ of the quotient ring $\mathbb{F}_q[X]/\langle X^n - \lambda \rangle$ is identified with a word $(a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}_q^n$. Any ideal C of $\mathbb{F}_q[X]/\langle X^n - \lambda \rangle$ is called a λ -constacyclic code of length n over \mathbb{F}_q . The 1-constacyclic codes are just the cyclic codes. The (-1) -constacyclic codes are also called *negacyclic codes*. If the greatest common divisor $\gcd(n, p) = 1$, then $X^n - \lambda$ has no repeated (multiple) roots and $\mathbb{F}_q[X]/\langle X^n - \lambda \rangle$ is a semisimple ring.

At the semisimple case, there are no self-dual cyclic codes. Leon, Masley and Pless [15] started the research on *duadic* and extended self-dual cyclic codes. Since then, duadic cyclic codes and various generalizations were investigated extensively, e.g., Pless [19], Smid [21], Rushanan [20], Ding and Pless [8] studied the duadic and extended self-dual cyclic codes. Brualdi and Pless [3], Ward

Email addresses: yfan@mail.ccnu.edu.cn (Y. Fan)

and Zhu [24], Ling and Xing [17], Sharma, Bakshi, Dumir and Raka [22] studied the polyadic cyclic or abelian codes. Williams [23], Matinnes-Pérez and Williams [18], Fan and Zhang [10], Jitman, Ling and Solé [14] studied self-dual or Hermitian self-dual group codes.

Dinh and Lopez-Permouth [7], Dinh [6] studied constacyclic codes; in particular, they showed that in the semisimple case self-duality happens for and only for negacyclic codes. Lim [16] studied polyadic consta-abelian codes. Blackford [1] gave conditions for the existence of the so-called *Type-I duadic* negacyclic codes. Chen, Fan, Lin and Liu [5] introduced a class of isometries to classify constacyclic codes. Blackford [2] introduced *isometrically self-dual* (“*iso-dual*” briefly) constacyclic codes, which are proved to be just the Type-I duadic constacyclic codes. Chen, Dinh, Fan and Ling [4] exhibited necessary and sufficient conditions for the existences of polyadic constacyclic codes. Fan and Zhang [11] classified the so-called *Type-II duadic* constacyclic codes which are in fact isometrically maximal self-orthogonal constacyclic codes. Note that most of the studies mentioned above considered the semisimple case; and, even in this case, there are less results on Hermitian self-dual constacyclic codes.

In this paper we study the duality and self-duality of constacyclic codes in a more general setting and by a uniform method. First, we consider any constacyclic codes, without the assumption “ $\gcd(n, p) = 1$ ”. Second, we define more general *isometries* between constacyclic codes which may be not semisimple. Third, we introduce a kind of inner products, called *Galois inner products*, as follows: for each integer h with $0 \leq h < e$ (recall that $q = p^e$), define:

$$\langle \mathbf{a}, \mathbf{b} \rangle_h = \sum_{i=0}^{n-1} a_i b_i^{p^h}, \quad \forall \mathbf{a} = (a_0, a_1, \dots, a_{n-1}), \mathbf{b} = (b_0, b_1, \dots, b_{n-1}) \in \mathbb{F}_q^n. \quad (1.1)$$

It is just the usual Euclidean inner product if $h = 0$. And, it is the Hermitian inner product if e is even and $h = \frac{e}{2}$. Then the *Galois dual codes* of constacyclic codes, the *Galois self-dual* (and *isometrically Galois self-dual*) constacyclic codes are naturally defined, which are investigated in this paper.

Since “ $p \mid n$ ” is allowed, constacyclic codes are no longer characterized by sets of zeros. In Section 2, we introduce so-called *q-coset functions* to characterize constacyclic codes.

We’ll study the *isometrically Galois self-dual* constacyclic codes in our general setting. So, in Section 3, we define the isometries between constacyclic codes in the general setting and explore their properties. The main result is Theorem 3.7 below.

In Section 4, with the isometries introduced in Section 3 we characterize the Galois dual codes of constacyclic codes by *q-coset functions*. The main result is Theorem 4.4 below. The results on dual and Hermitian dual codes are listed in Corollary 4.5 below.

In Section 5, a necessary and sufficient condition for the existence of isometrically Galois self-dual constacyclic codes is obtained, see Theorem 5.6 below,

which covers of course the isometrically self-dual case and the isometrically Hermitian self-dual case.

In Section 6, we study Galois self-dual constacyclic codes, and show a necessary and sufficient condition for their existence, see Theorem 6.4 below. The existence results on self-dual constacyclic codes and Hermitian self-dual constacyclic codes are drawn as consequences, see Corollary 6.5 and Corollary 6.6 below.

Finally, some examples are illustrated in Section 7.

2 Constacyclic codes and q -coset functions

In this paper we always take the following notations:

- \mathbb{F}_q denotes the finite field with cardinality $|\mathbb{F}_q| = q = p^e$, where p is a prime and e is a positive integer, and \mathbb{F}_q^* denotes the multiplicative group consisting of units of \mathbb{F}_q . So \mathbb{F}_q^* is a cyclic group of order $q - 1$.
- n is any positive integer, $\nu_p(n)$ denotes the p -adic valuation of n ; hence $n = p^{\nu_p(n)}n'$ with n' being coprime to p .
- $h \in [0, e]$, where $[0, e] = \{0, 1, \dots, e\}$ is an integer interval, and $\langle \mathbf{a}, \mathbf{b} \rangle_h = \sum_{i=0}^{n-1} a_i b_i^{p^h}$ as in Eqn (1.1).
- $\lambda \in \mathbb{F}_q^*$ with $\text{ord}_{\mathbb{F}_q^*}(\lambda) = r$, where $\text{ord}_{\mathbb{F}_q^*}(\lambda)$ denotes the order of λ in the group \mathbb{F}_q^* , hence $r \mid (q - 1)$.
- $R_{n,\lambda} = \mathbb{F}_q[X]/\langle X^n - \lambda \rangle$ is the quotient ring of the polynomial ring $\mathbb{F}_q[X]$ over \mathbb{F}_q with respect to the ideal $\langle X^n - \lambda \rangle$ generated by $X^n - \lambda$. By $C \leq R_{n,\lambda}$ we mean that C is an ideal of $R_{n,\lambda}$, i.e., C is a λ -constacyclic code of length n over \mathbb{F}_q .

Remark 2.1. By \mathbb{Z}_e we denote the residue ring of the integer ring \mathbb{Z} modulo e . Then the additive group of \mathbb{Z}_e is isomorphic to the Galois group of \mathbb{F}_q over \mathbb{F}_p by mapping $h \in \mathbb{Z}_e$ to the Galois automorphism γ_{p^h} of \mathbb{F}_q , where $\gamma_{p^h}(a) = a^{p^h}$ for all $a \in \mathbb{F}_q$. So, we call $\langle \mathbf{a}, \mathbf{b} \rangle_h$ a *Galois inner product* on \mathbb{F}_q^n .

Any element of the quotient ring $R_{n,\lambda}$ has a unique representative of degree at most $n - 1$: $a(X) = a_0 + a_1X + \dots + a_{n-1}X^{n-1}$. We always associate any word $a = (a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}_q^n$ with $a(X) = a_0 + a_1X + \dots + a_{n-1}X^{n-1}$ of the ring $R_{n,\lambda}$, and *vice versa*. Hence the Hamming weight $w(a(X))$ for $a(X) \in R_{n,\lambda}$ and the minimal weight $w(C)$ for $C \leq R_{n,\lambda}$ are defined as usual.

By Remark 2.1, there is a unique $\lambda' \in \mathbb{F}_q$ such that $\lambda = \gamma_{p^{\nu_p(n)}}(\lambda') = \lambda'^{p^{\nu_p(n)}}$, hence $\text{ord}_{\mathbb{F}_q^*}(\lambda') = \text{ord}_{\mathbb{F}_q^*}(\lambda) = r$. Note that $\gcd(q, n'r) = 1$, where $\gcd(-, -)$ denotes the greatest common divisor. In the following we always assume that:

- θ is a primitive $n'r$ -th root of unity in \mathbb{F}_{q^d} (with $d = \text{ord}_{\mathbb{Z}_{n'r}^*}(q)$) such that $\theta^{n'} = \lambda'$ (equivalently, $\theta^n = \lambda$), where $\mathbb{Z}_{n'r}^*$ denotes the multiplicative group consisting of units of the residue ring $\mathbb{Z}_{n'r}$.
- $1 + r\mathbb{Z}_{n'r}$ is the subset of $\mathbb{Z}_{n'r}$ as follows:

$$1 + r\mathbb{Z}_{n'r} = \{1 + rk \pmod{n'r} \mid k \in \mathbb{Z}_{n'r}\} = \{1, 1 + r, \dots, 1 + r(n' - 1)\}.$$

It is easy to check that θ^i for all $i \in (1 + r\mathbb{Z}_{n'r})$ are all roots of $X^{n'} - \lambda'$. In $\mathbb{F}_{q^d}[X]$ we have the following decomposition:

$$X^n - \lambda = (X^{n'} - \lambda')^{p^{\nu_p(n)}} = \prod_{i \in (1 + r\mathbb{Z}_{n'r})} (X - \theta^i)^{p^{\nu_p(n)}}. \quad (2.1)$$

Let s be an integer with $\gcd(s, n'r) = 1$. Then s induces a bijection

$$\mu_s : 1 + r\mathbb{Z}_{n'r} \rightarrow s + r\mathbb{Z}_{n'r}, \quad k \mapsto sk \pmod{n'r}, \quad (2.2)$$

where

$$s + r\mathbb{Z}_{n'r} = \{s + rk \pmod{n'r} \mid k \in \mathbb{Z}_{n'r}\}, \quad (2.3)$$

and θ^i for all $i \in (s + r\mathbb{Z}_{n'r})$ are all roots (with multiplicity $p^{\nu_p(n)}$) of $X^n - \lambda$.

It is easy to see that $s + r\mathbb{Z}_{n'r} = 1 + r\mathbb{Z}_{n'r}$ if and only if $s \equiv 1 \pmod{r}$. Assume that $s \equiv 1 \pmod{r}$. Then μ_s is a permutation of $1 + r\mathbb{Z}_{n'r}$. Any orbit of the permutation is called an s -orbit on $1 + r\mathbb{Z}_{n'r}$. In fact, for any integer t coprime to $n'r$, the μ_s (with $s \equiv 1 \pmod{r}$) is a permutation of the set $t + r\mathbb{Z}_{n'r}$, which is then partitioned into s -orbits.

Remark 2.2. (i) Since $r \mid (q - 1)$, we have $\gcd(q, n'r) = 1$ and $q \equiv 1 \pmod{r}$. The q -orbits on $1 + r\mathbb{Z}_{n'r}$ are also named q -cyclotomic cosets, or q -cosets in short. The quotient set consisting of q -cosets on $1 + r\mathbb{Z}_{n'r}$ is denoted by $(1 + r\mathbb{Z}_{n'r})/\mu_q$.

(ii) For an integer s with $\gcd(s, n'r) = 1$ and $s \equiv 1 \pmod{r}$, the permutation μ_s on $1 + r\mathbb{Z}_{n'r}$ induces a permutation, denote by μ_s again, of the quotient set $(1 + r\mathbb{Z}_{n'r})/\mu_q$, and partitions the quotient set into s -orbits; cf [4, Lemma 8]. That is, for any $Q \in (1 + r\mathbb{Z}_{n'r})/\mu_q$, $sQ = \{sk \mid k \in Q\}$ is still a q -coset, and there is a positive integer ℓ such that $s^i Q \neq s^j Q$ if $0 \leq i \neq j < \ell$, but $s^\ell Q = Q$; then $Q, sQ, \dots, s^{\ell-1}Q$ form an s -orbit of length ℓ on the quotient set.

Example 7.4 in Section 7 is a non-trivial example for the above notations.

Then we further define the polynomials $f_Q(X)$ for q -cosets Q 's and get a decomposition as follows:

$$X^n - \lambda = \prod_{Q \in (1 + r\mathbb{Z}_{n'r})/\mu_q} f_Q(X)^{p^{\nu_p(n)}} \quad \text{where } f_Q(X) = \prod_{i \in Q} (X - \theta^i), \quad (2.4)$$

and $f_Q(X)$ for all $Q \in (1 + r\mathbb{Z}_{n'r})/\mu_q$ are irreducible \mathbb{F}_q -polynomials.

Definition 2.3. Let $[0, p^{\nu_p(n)}]$ be the integer interval $\{0, 1, \dots, p^{\nu_p(n)}\}$.

- (i) A map $\varphi : 1 + r\mathbb{Z}_{n'r} \rightarrow [0, p^{\nu_p(n)}]$ is called a *q-coset function* if for any $k \in 1 + r\mathbb{Z}_{n'r}$ and any integer i we have $\varphi(q^i k) = \varphi(k)$. Thus, any *q-coset function* $\varphi : 1 + r\mathbb{Z}_{n'r} \rightarrow [0, p^{\nu_p(n)}]$ is identified with a function (denoted by φ again) on the quotient set:

$$\varphi : (1 + r\mathbb{Z}_{n'r})/\mu_q \rightarrow [0, p^{\nu_p(n)}], \quad Q \mapsto \varphi(Q), \quad \text{where } \varphi(Q) = \varphi(k) \text{ for } k \in Q;$$

then a polynomial $f_\varphi(X) \in \mathbb{F}_q[X]$ can be defined as follows:

$$f_\varphi(X) = \prod_{Q \in (1 + r\mathbb{Z}_{n'r})/\mu_q} f_Q(X)^{\varphi(Q)}.$$

- (ii) For any *q-coset function* $\varphi : 1 + r\mathbb{Z}_{n'r} \rightarrow [0, p^{\nu_p(n)}]$, we define a function $\bar{\varphi} : 1 + r\mathbb{Z}_{n'r} \rightarrow [0, p^{\nu_p(n)}]$ by $\bar{\varphi}(k) = p^{\nu_p(n)} - \varphi(k)$. The function $\bar{\varphi}$ is also a *q-coset function*, which we call by the *complement of φ* .
- (iii) For any integer s coprime to $n'r$ and any *q-coset function* $\varphi : 1 + r\mathbb{Z}_{n'r} \rightarrow [0, p^{\nu_p(n)}]$, define a function $s\varphi : s + r\mathbb{Z}_{n'r} \rightarrow [0, p^{\nu_p(n)}]$ by

$$(s\varphi)(k) = \varphi(s^{-1}k), \quad \forall k \in s + r\mathbb{Z}_{n'r}.$$

where s^{-1} is an integer such that $s^{-1}s \equiv 1 \pmod{n'r}$. It is easy to check that $s\varphi$ is still a *q-coset function*.

- (iv) Let $\varphi, \varphi' : 1 + r\mathbb{Z}_{n'r} \rightarrow [0, p^{\nu_p(n)}]$ be *q-coset functions*. Define

$$(\varphi \cap \varphi')(k) = \min\{\varphi(k), \varphi'(k)\}, \quad \forall k \in 1 + r\mathbb{Z}_{n'r}.$$

The function $\varphi \cap \varphi'$ is clearly a *q-coset function* too. Further, if $\varphi \cap \varphi' = \varphi$, then we write $\varphi \leq \varphi'$.

By Eqn (2.4) and the definition of $\varphi \cap \bar{\varphi}$, we have

$$f_\varphi(X)f_{\bar{\varphi}}(X) = X^n - \lambda, \quad \gcd(f_\varphi(X), f_{\bar{\varphi}}(X)) = f_{\varphi \cap \bar{\varphi}}(X). \quad (2.5)$$

It is a routine to verify the following two lemmas.

Lemma 2.4. *For any λ -constacyclic code $C \leq R_{n,\lambda}$ there is exactly one *q-coset function* $\varphi : (1 + r\mathbb{Z}_{n'r})/\mu_q \rightarrow [0, p^{\nu_p(n)}]$ satisfying the following:*

- (i) $c(X) \in C$ if and only if $c(X)f_\varphi(X) \equiv 0 \pmod{X^n - \lambda}$.
- (ii) $c(X) \in C$ if and only if $f_{\bar{\varphi}}(X) \mid c(X)$.

Definition 2.5. As usual, $f_\varphi(X)$ in Lemma 2.4 is called a *check polynomial* of the λ -constacyclic code C , and $f_{\bar{\varphi}}(X)$ is called a *generator polynomial* of C . Because of the uniqueness of the *q-coset function* φ , we denote the λ -constacyclic code C by C_φ , and call it the λ -constacyclic code with check polynomial $f_\varphi(X)$.

For any $C \leq R_{n,\lambda}$, we set

$$\text{Ann}(C) = \{a(X) \in R_{n,\lambda} \mid a(X)c(X) \equiv 0 \pmod{X^n - \lambda}, \forall c(X) \in C\}. \quad (2.6)$$

which is an ideal of $R_{n,\lambda}$, i.e., is a λ -constacyclic code too.

Lemma 2.6. *Let $C_\varphi \leq R_{n,\lambda}$, where $\varphi : (1 + r\mathbb{Z}_{n'r})/\mu_q \rightarrow [0, p^{\nu_p(n)}]$ is a q -coset function. Then $\text{Ann}(C_\varphi) = C_{\bar{\varphi}}$.*

3 Ring isometries

For any non-zero integer s , by $\nu_p(s)$ we denote the p -adic valuation of s , hence $s = p^{\nu_p(s)}s'$ with $p \nmid s'$. If $\gcd(s, n'r) = 1$ then $\gcd(s', nr) = 1$ obviously.

Theorem 3.1. *Assume that $\gcd(s, n'r) = 1$, $s = p^{\nu_p(s)}s'$ and s'^{-1} is an integer such that $s'^{-1}s' \equiv 1 \pmod{nr}$. Then the map $\mathcal{M}_s : R_{n,\lambda} \rightarrow R_{n,\lambda^s}$ defined by*

$$\mathcal{M}_s\left(\sum_{i=0}^{n-1} a_i X^i\right) = \sum_{i=0}^{n-1} a_i^{p^{\nu_p(s)}} X^{is'^{-1}} \pmod{X^n - \lambda^s}, \quad \forall \sum_{i=0}^{n-1} a_i X^i \in R_{n,\lambda}, \quad (3.1)$$

is well-defined (independent of the choice of s'^{-1}) and the following hold:

- (i) \mathcal{M}_s is a ring isomorphism.
- (ii) $w(\mathcal{M}_s(a(X))) = w((a(X)))$ for all $a(X) \in R_{n,\lambda}$.

Proof. Mapping a to $a^{p^{\nu_p(s)}}$ is an automorphism of \mathbb{F}_q , see Remark 2.1. It is obvious that the following map

$$\mathbb{F}_q[X] \rightarrow \mathbb{F}_q[X], \quad \sum_{i=0}^k a_i X^i \mapsto \sum_{i=0}^k a_i^{p^{\nu_p(s)}} X^{is'^{-1}}$$

is a ring homomorphism; hence it induces a ring homomorphism:

$$\begin{aligned} \widehat{\mathcal{M}}_s : \mathbb{F}_q[X] &\rightarrow \mathbb{F}_q[X]/\langle X^n - \lambda^s \rangle, \\ \sum_{i=0}^k a_i X^i &\rightarrow \sum_{i=0}^k a_i^{p^{\nu_p(s)}} X^{is'^{-1}} \pmod{X^n - \lambda^s}. \end{aligned}$$

In the ring $R_{n,\lambda^s} = \mathbb{F}_q[X]/\langle X^n - \lambda^s \rangle$ we have the following computation:

$$\widehat{\mathcal{M}}_s(X^n - \lambda) = X^{ns'^{-1}} - \lambda^{p^{\nu_p(s)}} \equiv (\lambda^{p^{\nu_p(s)}s'})^{s'^{-1}} - \lambda^{p^{\nu_p(s)}} = 0 \pmod{X^n - \lambda^s}.$$

Thus the ring homomorphism $\widehat{\mathcal{M}}_s$ induces a well-defined ring homomorphism as follows:

$$\begin{aligned} \mathcal{M}_s : \mathbb{F}_q[X]/\langle X^n - \lambda \rangle &\rightarrow \mathbb{F}_q[X]/\langle X^n - \lambda^s \rangle, \\ \sum_{i=0}^{n-1} a_i X^i &\rightarrow \sum_{i=0}^{n-1} a_i^{p^{\nu_p(s)}} X^{is'^{-1}} \pmod{X^n - \lambda^s}. \end{aligned}$$

Because s'^{-1} is unique modulo nr and $\lambda^{nr} = 1$, \mathcal{M}_s is independent of the choice of the integer s'^{-1} such that $s'^{-1}s' \equiv 1 \pmod{nr}$. Since $\gcd(s'^{-1}, n) = 1$, for any j we can find an i such that $is'^{-1} \equiv j \pmod{n}$, i.e., $is'^{-1} = nt + j$ for an integer t . Further, there is an $a \in \mathbb{F}_q$ such that $a^{p^{\nu_p(s)}} = \lambda^{-st}$. Then in the ring $\mathbb{F}_q[X]/\langle X^n - \lambda^s \rangle$ we have

$$\mathcal{M}_s(aX^i) = a^{p^{\nu_p(s)}} X^{is'^{-1}} \equiv a^{p^{\nu_p(s)}} \lambda^{st} X^j = X^j \pmod{X^n - \lambda^s}.$$

Thus the ring homomorphism \mathcal{M}_s is surjective. Further, the cardinalities of $\mathbb{F}_q[X]/\langle X^n - \lambda \rangle$ and $\mathbb{F}_q[X]/\langle X^n - \lambda^s \rangle$ are equal to each other. So \mathcal{M}_s is a ring isomorphism, i.e., (i) holds. Finally, (ii) holds obviously. \square

Remark 3.2. We call the \mathcal{M}_s defined in Theorem 3.1 a *ring isometry* from $R_{n,\lambda}$ to R_{n,λ^s} . Note that the isometries between constacyclic codes appeared in literature, e.g., in [5, 2, 4, 11], are defined only for the semisimple case (i.e., $\gcd(n, q) = 1$) and are algebra isomorphism. The ring isometries \mathcal{M}_s in Theorem 3.1 are defined for the general case (where “ $p|n$ ” is allowed), and are semi-linear algebra isomorphisms in general, i.e., they are isomorphisms of rings and semi-linear isomorphisms of vector spaces. Precisely, \mathcal{M}_s is a $\gamma_{p^{\nu_p(s)}}$ -linear isomorphism, where $\gamma_{p^{\nu_p(s)}}$ is the Galois automorphism defined in Remark 2.1. For any constacyclic code $C \leq R_{n,\lambda}$, by the semi-linearity of \mathcal{M}_s , we still have $\dim_{\mathbb{F}_q}(\mathcal{M}_s(C)) = \dim_{\mathbb{F}_q}(C)$.

Lemma 3.3. *Let s_1 and s_2 be integers coprime to $n'r$, let $s_1 = p^{\nu_p(s_1)}s'_1$ and $s_2 = p^{\nu_p(s_2)}s'_2$. Then the following two are equivalent:*

- (i) $\mathcal{M}_{s_1} = \mathcal{M}_{s_2}$.
- (ii) $s'_1 \equiv s'_2 \pmod{nr}$ and $\nu_p(s_1) \equiv \nu_p(s_2) \pmod{e}$.

Proof. Let $s_1'^{-1}, s_2'^{-1}$ be integers with $s_1'^{-1}s'_1 \equiv 1 \pmod{nr}$, $s_2'^{-1}s'_2 \equiv 1 \pmod{nr}$. Suppose that $\mathcal{M}_{s_1} = \mathcal{M}_{s_2}$. Then $\lambda^{s_1} = \lambda^{s_2}$, hence $s_1 \equiv s_2 \pmod{r}$. And, $\mathcal{M}_{s_1}(X) = \mathcal{M}_{s_2}(X)$, i.e., $X^{s_1'^{-1}} \equiv X^{s_2'^{-1}} \pmod{X^n - \lambda^{s_1}}$. Let $s_i'^{-1} = t_i n + k_i$ with $0 \leq k_i < n$ for $i = 1, 2$. Then $X^{s_i'^{-1}} \equiv \lambda^{s_1 t_i} X^{k_i} \pmod{X^n - \lambda^{s_1}}$. We get that $\lambda^{s_1 t_1} X^{k_1} = \lambda^{s_1 t_2} X^{k_2}$. Then $t_1 \equiv t_2 \pmod{r}$ and $k_1 = k_2$, which imply that $s_1'^{-1} \equiv s_2'^{-1} \pmod{nr}$, equivalently, $s'_1 \equiv s'_2 \pmod{nr}$. Further, $\mathcal{M}_{s_1}(a) = \mathcal{M}_{s_2}(a)$ for any $a \in \mathbb{F}_q$. Then $a^{p^{\nu_p(s_1)}} = a^{p^{\nu_p(s_2)}}$ for any $a \in \mathbb{F}_q$; so $\nu_p(s_1) \equiv \nu_p(s_2) \pmod{e}$, cf. Remark 2.1. The necessity is proved. The sufficiency is obvious. \square

It is easy to see that

$$\mathcal{M}_{s_1}\mathcal{M}_{s_2} = \mathcal{M}_{s_1 s_2}, \quad \text{for } s_1, s_2 \text{ coprime to } n'r. \quad (3.2)$$

Lemma 3.3 implies that the set of ring isometries $\{\mathcal{M}_s \mid s \text{ is coprime to } n'r\}$ form a group which is isomorphic to $\mathbb{Z}_e \times \mathbb{Z}_{n'r}^*$.

Remark 3.4. We know that $\lambda^s = \lambda$ if and only if $s \equiv 1 \pmod{r}$. So $R_{n,\lambda^s} = R_{n,\lambda}$ if and only if $s \in 1 + r\mathbb{Z}_{n'r}$. At that case, for any $Q \in (1 + r\mathbb{Z}_{n'r})/\mu_q$, $sQ = \{sk \mid k \in Q\}$ is still a q -coset on $1 + r\mathbb{Z}_{n'r}$. However, if $s \not\equiv 1 \pmod{r}$, then θ^i for $i \in s + r\mathbb{Z}_{n'r}$ are all roots of $X^{n'} - \lambda'^s$, cf. Eqn (2.3). And, a μ_q -action on $s + r\mathbb{Z}_{n'r}$ is defined the same as in Eqn (2.2) so that, for any $Q \in (1 + r\mathbb{Z}_{n'r})/\mu_q$, the sQ is a q -coset on $s + r\mathbb{Z}_{n'r}$; cf. Remark 2.2. Thus $Q \mapsto sQ$ is a bijective map from $(1 + r\mathbb{Z}_{n'r})/\mu_q$ onto $(s + r\mathbb{Z}_{n'r})/\mu_q$; the converse map sends any q -coset $Q' \in (s + r\mathbb{Z}_{n'r})/\mu_q$ to $s^{-1}Q' = \{s^{-1}k' \mid k' \in Q'\}$, where $s^{-1}s \equiv 1 \pmod{n'r}$ as in Definition 2.3 (iii).

Lemma 3.5. *Let s be an integer coprime to $n'r$. Then for any q -coset $Q \in (1 + r\mathbb{Z}_{n'r})/\mu_q$ there is a unit $u(X) \in R_{n,\lambda^s}$ such that*

$$\mathcal{M}_s(f_Q(X)) = u(X)f_{sQ}(X).$$

Proof. Let $s = p^{\nu_p(s)}s'$ and s'^{-1} be an integer such that $s'^{-1}s' \equiv 1 \pmod{nr}$. Note that $f_Q(X) = \prod_{i \in Q} (X - \theta^i)$, see Eqn (2.4), and \mathcal{M}_s is a ring isomorphism, see Theorem 3.1. So

$$\begin{aligned} \mathcal{M}_s(f_Q(X)) &= \prod_{i \in Q} (X^{s'^{-1}} - \theta^{ip^{\nu_p(s)}}) = \prod_{i \in Q} (X^{s'^{-1}} - (\theta^{is})^{s'^{-1}}) \\ &= \left(\prod_{i \in Q} (X - \theta^{is}) \right) \left(\prod_{i \in Q} \frac{X^{s'^{-1}} - (\theta^{is})^{s'^{-1}}}{X - \theta^{is}} \right) \\ &= \left(\prod_{j \in sQ} (X - \theta^j) \right) \left(\prod_{i \in Q} \frac{X^{s'^{-1}} - (\theta^{is})^{s'^{-1}}}{X - \theta^{is}} \right) \\ &= f_{sQ}(X) \cdot u(X), \end{aligned}$$

where $u(X) = \prod_{i \in Q} \frac{X^{s'^{-1}} - (\theta^{is})^{s'^{-1}}}{X - \theta^{is}}$. It is enough to show that $u(X)$ is coprime

to $X^n - \lambda^s$. Further, it is enough to show that, for any $i \in Q$, $\frac{X^{s'^{-1}} - (\theta^{is})^{s'^{-1}}}{X - \theta^{is}}$ is coprime to $X^n - \lambda^s$. Note that θ^{js} for $j \in 1 + r\mathbb{Z}_{n'r}$ are all roots of $X^n - \lambda^s$, cf. Eqn (2.3) and Remark 3.4. If $j \not\equiv i \pmod{n'r}$, then $jss'^{-1} \not\equiv iss'^{-1} \pmod{n'r}$ because ss'^{-1} is coprime to $n'r$, hence $(\theta^{js})^{s'^{-1}} - (\theta^{is})^{s'^{-1}} \neq 0$. So, any root θ^{js} of $X^n - \lambda^s$ for $j \in 1 + r\mathbb{Z}_{n'r}$ is not a root of the polynomial $\frac{X^{s'^{-1}} - (\theta^{is})^{s'^{-1}}}{X - \theta^{is}}$. This completes the proof of the lemma. \square

Lemma 3.6. *Let s be an integer coprime to $n'r$, and $\varphi : 1 + r\mathbb{Z}_{n'r} \rightarrow [0, p^{\nu_p(n)}]$ be a q -coset function. Then there is a unit $u(X) \in R_{n,\lambda^s}$ such that*

$$\mathcal{M}_s(f_\varphi(X)) = u(X)f_{s\varphi}(X).$$

Proof. Since $f_\varphi(X) = \prod_{Q \in (1 + r\mathbb{Z}_{n'r})/\mu_q} f_Q(X)^{\varphi(Q)}$, see Definition 2.3 (i), and \mathcal{M}_s is a ring isomorphism, we have:

$$\mathcal{M}_s(f_\varphi(X)) = \prod_{Q \in (1 + r\mathbb{Z}_{n'r})/\mu_q} \mathcal{M}_s(f_Q(X))^{\varphi(Q)}.$$

For each $Q \in (1 + r\mathbb{Z}_{n'r})/\mu_q$, by Lemma 3.5 we have a unit $u_Q(X)$ in R_{n,λ^s} such that $\mathcal{M}_s(f_Q(X)) = u_Q(X)f_{sQ}(X)$. Then $u(X) = \prod_{Q \in (1+r\mathbb{Z}_{n'r})/\mu_q} u_Q(X)$ is a unit of R_{n,λ^s} and

$$\mathcal{M}_s(f_\varphi(X)) = u(X) \prod_{Q \in (1+r\mathbb{Z}_{n'r})/\mu_q} f_{sQ}(X)^{\varphi(Q)}.$$

As mentioned in Remark 3.4, sQ runs over $(s + r\mathbb{Z}_{n'r})/\mu_q$ when Q runs over $(1 + r\mathbb{Z}_{n'r})/\mu_q$; conversely, $s^{-1}Q'$ runs over $(1 + r\mathbb{Z}_{n'r})/\mu_q$ when Q' runs over $(s + r\mathbb{Z}_{n'r})/\mu_q$. Thus, we get

$$\mathcal{M}_s(f_\varphi(X)) = u(X) \prod_{Q' \in (s+r\mathbb{Z}_{n'r})/\mu_q} f_{Q'}(X)^{\varphi(s^{-1}Q')}.$$

But $\varphi(s^{-1}Q') = s\varphi(Q')$, see Definition 2.3 (iii). So

$$\mathcal{M}_s(f_\varphi(X)) = u(X) \prod_{Q' \in (s+r\mathbb{Z}_{n'r})/\mu_q} f_{Q'}(X)^{(s\varphi)(Q')};$$

that is, $\mathcal{M}_s(f_\varphi(X)) = u(X)f_{s\varphi}(X)$. □

As a consequence, we obtain the following immediately.

Theorem 3.7. *Let s be an integer coprime to $n'r$, and $\varphi : 1 + r\mathbb{Z}_{n'r} \rightarrow [0, p^{\nu_p(n)}]$ be a q -coset function. Then $\mathcal{M}_s(C_\varphi) = C_{s\varphi}$ which is a λ^s -constacyclic code.*

By Theorem 3.7 and Lemma 3.3, we get the following at once.

Corollary 3.8. *Let s_1 and s_2 be integers coprime to $n'r$, let $s_1 = p^{\nu_p(s_1)}s'_1$ and $s_2 = p^{\nu_p(s_2)}s'_2$. Then the following two are equivalent to each other:*

- (i) $s_1\varphi = s_2\varphi$, for any q -coset function $\varphi : 1 + r\mathbb{Z}_{n'r} \rightarrow [0, p^{\nu_p(n)}]$.
- (ii) $s'_1 \equiv s'_2 \pmod{nr}$ and $\nu_p(s_1) \equiv \nu_p(s_2) \pmod{e}$.

4 Galois dual codes of constacyclic codes

Definition 4.1. For $h \in [0, e]$, the Galois inner product $\langle \mathbf{a}, \mathbf{b} \rangle_h = \sum_{i=0}^{n-1} a_i b_i^{p^h}$ is defined in Eqn (1.1), which we call explicitly the p^h -inner product. For any code $C \subseteq \mathbb{F}_q^n$ we have a code $C^{\perp h} = \{\mathbf{a} \in \mathbb{F}_q^n \mid \langle \mathbf{c}, \mathbf{a} \rangle_h = 0, \forall \mathbf{c} \in C\}$, and call it the *Galois dual-code* (more explicitly, the p^h -dual code) of the code C .

Remark 4.2. Obviously, $\langle \mathbf{a}, \mathbf{b} \rangle_h$ is a non-degenerate form on \mathbb{F}_q^n ; it is a linear function for the first variable \mathbf{a} , while it is a semi-linear function for the second variable \mathbf{b} ; more precisely, it is γ_{p^h} -linear for the second variable \mathbf{b} , where γ_{p^h}

is the Galois automorphism of the field \mathbb{F}_q defined in Remark 2.1. In particular, if $C \subseteq \mathbb{F}_q^n$ is a linear code, then $\dim_{\mathbb{F}_q}(C) + \dim_{\mathbb{F}_q}(C^{\perp h}) = n$.

The p^0 -inner product $\langle \mathbf{a}, \mathbf{b} \rangle_0$ is the Euclidean inner product and $C^{\perp 0}$ is just the usual dual code of C . The $p^{\frac{e}{2}}$ -inner product $\langle \mathbf{a}, \mathbf{b} \rangle_{\frac{e}{2}}$ (if e is even) is the Hermitian inner product and $C^{\perp \frac{e}{2}}$ is just the Hermitian dual code of C .

In this section we characterize the Galois dual codes of constacyclic codes by q -coset functions.

Lemma 4.3. *Let $C \subseteq R_{n,\lambda}$ be a code, let $\text{Ann}(C)$ be as in Eqn (2.6). Then*

$$C^{\perp h} = \mathcal{M}_{-p^{e-h}}(\text{Ann}(C)).$$

In particular, $C^{\perp h}$ is a $\lambda^{-p^{e-h}}$ -constacyclic code.

Proof. Assume $a(X) = \sum_{i=0}^{n-1} a_i X^i$, $b(X) = \sum_{i=0}^{n-1} b_i X^i$. In the ring $R_{n,\lambda}$ we have the following computation:

$$\begin{aligned} a(X)b(X) &= \sum_{k=0}^{n-1} \sum_{i+j=k} a_i b_j X^k + \sum_{k=n}^{2n-2} \sum_{i+j=k} a_i b_j X^k \\ &\equiv \sum_{k=0}^{n-1} \left(\sum_{i+j=k} a_i b_j + \sum_{i+j=n+k} \lambda a_i b_j \right) X^k \pmod{X^n - \lambda}. \end{aligned}$$

Thus

$$a(X)b(X) \equiv 0 \pmod{X^n - \lambda}$$

if and only if

$$\sum_{i=0}^k a_i b_{k-i} + \lambda \sum_{i=k+1}^{n-1} a_i b_{k+n-i} = 0, \quad k = 0, 1, \dots, n-1. \quad (4.1)$$

In $R_{n,\lambda^{-p^{e-h}}} = \mathbb{F}_q[X]/\langle X^n - \lambda^{-p^{e-h}} \rangle$, consider the ideal $\langle \mathcal{M}_{-p^{e-h}}(b(X)) \rangle$ generated by the polynomial $\mathcal{M}_{-p^{e-h}}(b(X))$. Since

$$\lambda^{p^{e-h}} X^n \equiv 1 \pmod{X^n - \lambda^{-p^{e-h}}},$$

for $0 \leq k \leq n$, X^k is a unit of $R_{n,\lambda^{-p^{e-h}}}$, $X^k \mathcal{M}_{-p^{e-h}}(b(X))$ is a generator of the ideal $\langle \mathcal{M}_{-p^{e-h}}(b(X)) \rangle$ and

$$\begin{aligned} X^k \mathcal{M}_{-p^{e-h}}(b(X)) &= X^k \sum_{j=0}^{n-1} b_j^{p^{e-h}} X^{-j} \\ &\equiv \sum_{j=0}^k b_j^{p^{e-h}} X^{k-j} + \lambda^{p^{e-h}} \sum_{j=k+1}^{n-1} b_j^{p^{e-h}} X^{n+k-j} \pmod{X^n - \lambda^{-p^{e-h}}}. \end{aligned}$$

In the right hand side, we replace $k-j$ by i in the first \sum , and replacing $n+k-j$ by i in the second \sum . In the ring $R_{n,\lambda^{-p^{e-h}}}$, we get that

$$X^k \mathcal{M}_{-p^{e-h}}(b(X)) = \sum_{i=0}^k b_{k-i}^{p^{e-h}} X^i + \lambda^{p^{e-h}} \sum_{i=k+1}^{n-1} b_{n+k-i}^{p^{e-h}} X^i, \quad k = 0, 1, \dots, n-1. \quad (4.2)$$

Note that $(f^{p^{e-h}})^{p^h} = f$ for any $f \in \mathbb{F}_q$. From Eqn (4.1) and Eqn (4.2) we obtain that

$$a(X)b(X) = 0 \text{ in } R_{n,\lambda} \iff \langle \mathcal{M}_{-p^{e-h}}(b(X)) \rangle \subseteq a(X)^{\perp h} \text{ in } R_{n,\lambda^{-p^{e-h}}}.$$

Thus

$$\mathcal{M}_{-p^{e-h}}(\text{Ann}(C)) \subseteq C^{\perp h}.$$

The inclusion has to be an equality because $\dim_{\mathbb{F}_q}(C^{\perp}) = \dim_{\mathbb{F}_q}(\text{Ann}(C))$. \square

Combining the above lemma with Lemma 2.6 and Theorem 3.7, we get the following theorem and corollary at once.

Theorem 4.4. *Let $C_\varphi \leq R_{n,\lambda}$ be a λ -constacyclic code with check polynomial $f_\varphi(X)$, where $\varphi : (1 + r\mathbb{Z}_{n'r})/\mu_q \rightarrow [0, p^{\nu_p(n)}]$ is a q -coset function. Then*

$$C_\varphi^{\perp h} = \mathcal{M}_{-p^{e-h}}(C_{\bar{\varphi}}) = C_{-p^{e-h}\bar{\varphi}}$$

which is a $\lambda^{-p^{e-h}}$ -constacyclic code.

Corollary 4.5. (i) *The dual code $C_\varphi^{\perp 0} = C_{-\bar{\varphi}}$, which is a λ^{-1} -constacyclic code.*

(ii) *The Hermitian dual code $C_\varphi^{\perp \frac{e}{2}} = C_{-p^{\frac{e}{2}}\bar{\varphi}}$, which is a $\lambda^{-p^{\frac{e}{2}}}$ -constacyclic code.*

In the semisimple case (i.e. $\nu_p(n) = 0$), the conclusion (i) of the corollary was proved in [2]. On the other hand, it has been shown in [6, 14] that the Hermitian dual code of a λ -constacyclic code is a $\lambda^{-p^{\frac{e}{2}}}$ -constacyclic code.

5 Isometrically Galois self-dual constacyclic codes

Definition 5.1. Let $C_\varphi \leq R_{n,\lambda}$ be a λ -constacyclic code with check polynomial $f_\varphi(X)$, where $\varphi : (1 + r\mathbb{Z}_{n'r})/\mu_q \rightarrow [0, p^{\nu_p(n)}]$ is a q -coset function.

(i) If $C_\varphi = C_\varphi^{\perp h}$, then we say that C_φ is a *Galois self-dual* (more explicitly, *p^h -self-dual*) λ -constacyclic code.

(ii) If there is an integer s with $\gcd(s, n'r) = 1$ and $s \equiv 1 \pmod{r}$ such that

$$\mathcal{M}_{-p^{e-h}s}(C_\varphi) = C_\varphi^{\perp h},$$

then we say that C_φ is *isometrically Galois self-dual* (more explicitly, *isometrically p^h -self-dual*).

The p^0 -self-dual constacyclic codes are just the usual self-dual constacyclic codes, which were studied by many researchers, e.g., [1, 7, 8]. The isometrically p^0 -self-dual constacyclic codes are the so-called iso-dual constacyclic codes studied in [2]. And, the $p^{\frac{e}{2}}$ -self-dual constacyclic codes (if e is even) are the usual Hermitian self-dual constacyclic codes considered in [2].

Recall that a linear code is said to be *formal self-dual* if the code and its dual code have one and the same weight distribution, cf. [13, p.307]. Any isometrically Galois self-dual constacyclic code is obviously formal self-dual.

In this section we'll exhibit a necessary and sufficient condition for the existence of isometrically Galois self-dual constacyclic codes.

Lemma 5.2. *Let s be an integer with $\gcd(s, n'r) = 1$ and $s \equiv 1 \pmod{r}$. Let $\varphi : (1 + r\mathbb{Z}_{n'r})/\mu_q \rightarrow [0, p^{\nu_p(n)}]$ be a q -coset function. Then the following four statements are equivalent to each other:*

- (i) $\mathcal{M}_{-p^{e-h}s}(C_\varphi) = C_\varphi^{\perp h}$.
- (ii) $s\varphi = \bar{\varphi}$.
- (iii) $\varphi(Q) + \varphi(sQ) = p^{\nu_p(n)}, \forall Q \in (1 + r\mathbb{Z}_{n'r})/\mu_q$.
- (iv) For any s -orbit $Q, sQ, \dots, s^{\ell-1}Q$ of length ℓ on $(1 + r\mathbb{Z}_{n'r})/\mu_q$ (see Remark 2.2 (ii)), one of the following two holds:
 - (iv.a) ℓ is even, $\varphi(Q) = \varphi(s^2Q) = \dots = \varphi(s^{\ell-2}Q)$, $\varphi(sQ) = \varphi(s^3Q) = \dots = \varphi(s^{\ell-1}Q)$, and $\varphi(Q) + \varphi(sQ) = p^{\nu_p(n)}$.
 - (iv.b) ℓ is odd, $\varphi(Q) = \varphi(sQ) = \varphi(s^2Q) = \dots = \varphi(s^{\ell-1}Q) = \frac{1}{2}p^{\nu_p(n)}$.

Proof. (i) \iff (ii). By Theorem 4.4, $C_\varphi^{\perp h} = C_{-p^{e-h}s\varphi}$. On the other hand, by Theorem 3.7, $\mathcal{M}_{-p^{e-h}s}(C_\varphi) = C_{-p^{e-h}s\varphi}$. So $\mathcal{M}_{-p^{e-h}s}(C_\varphi) = C_\varphi^{\perp h}$ if and only if $C_{-p^{e-h}s\varphi} = C_{-p^{e-h}\bar{\varphi}}$, if and only if $-p^{e-h}s\varphi = -p^{e-h}\bar{\varphi}$. Note that $-p^{e-h} \in \mathbb{Z}_{n'r}^*$. So $-p^{e-h}s\varphi = -p^{e-h}\bar{\varphi}$ if and only if $s\varphi = \bar{\varphi}$.

(ii) \iff (iii). Let s be an integer such that $s^{-1}s \equiv 1 \pmod{n'r}$, let $Q \in (1 + r\mathbb{Z}_{n'r})/\mu_q$. (ii) can be rewritten as $\varphi = s^{-1}\bar{\varphi}$. If it holds, then $\varphi(Q) = s^{-1}\bar{\varphi}(Q) = \bar{\varphi}(sQ) = p^{\nu_q(n)} - \varphi(sQ)$, see Definition 2.3; i.e., (iii) holds. If (iii) holds, then $\varphi(Q) = p^{\nu_q(n)} - \varphi(sQ) = \bar{\varphi}(sQ) = s^{-1}\bar{\varphi}(Q)$, i.e., (ii) holds.

(iii) \implies (iv). By (iii), $\varphi(Q) + \varphi(sQ) = p^{\nu_p(n)} = \varphi(sQ) + \varphi(s^2Q)$. We get $\varphi(Q) = \varphi(s^2Q)$. Similarly, $\varphi(sQ) + \varphi(s^2Q) = \varphi(s^2Q) + \varphi(s^3Q)$. we get $\varphi(sQ) = \varphi(s^3Q)$. Iterating in this way, we see that

$$\varphi(s^i Q) = \begin{cases} \varphi(Q), & i \text{ is even;} \\ \varphi(sQ), & i \text{ is odd.} \end{cases} \quad (5.1)$$

If ℓ is even, then, noting that $\ell - 2$ is even while $\ell - 1$ is odd, we get:

$$\varphi(Q) = \varphi(s^2Q) = \dots = \varphi(s^{\ell-2}Q), \quad \varphi(sQ) = \varphi(s^3Q) = \dots = \varphi(s^{\ell-1}Q).$$

Otherwise, ℓ is odd. Since $s^\ell Q = Q$ (see Remark 2.2 (ii)), by Eqn (5.1) we obtain that

$$\varphi(sQ) = \varphi(s^\ell Q) = \varphi(Q).$$

Combining it with (iii), we further get that $\varphi(Q) = \varphi(sQ) = \frac{1}{2}p^{\nu_p(n)}$. By Eqn (5.1), $\varphi(s^i Q) = \frac{1}{2}p^{\nu_p(n)}$ for any integer i .

(iv) \implies (iii). Obviously, (iv) implies that, for any s -orbit $Q, sQ, \dots, s^{\ell-1}Q$ of length ℓ on $(1 + r\mathbb{Z}_{n'r})/\mu_q$, we have

$$\varphi(s^i Q) + \varphi(s^{i+1} Q) = p^{\nu_p(n)}, \quad i = 0, 1, \dots.$$

Thus, (iii) holds. \square

A characterization of isometrically p^h -self-dual constacyclic codes by q -coset functions is obviously obtained as follows.

Corollary 5.3. C_φ is isometrically p^h -self-dual if and only if there is an integer s with $\gcd(s, n'r) = 1$ and $s \equiv 1 \pmod{r}$ such that $s\varphi = \bar{\varphi}$.

Lemma 5.4. Let s be an integer with $\gcd(s, n'r) = 1$ and $s \equiv 1 \pmod{r}$. The following two statements are equivalent to each other:

- (i) There exists a q -coset function $\varphi : (1 + r\mathbb{Z}_{n'r})/\mu_q \rightarrow [0, p^{\nu_p(n)}]$ such that $s\varphi = \bar{\varphi}$.
- (ii) One of the following two conditions holds:
 - (ii.1) $p = 2$ and $\nu_2(n) \geq 1$.
 - (ii.2) The length of any s -orbit on $(1 + r\mathbb{Z}_{n'r})/\mu_q$ is even.

Proof. (i) \implies (ii). Assume that (i) holds and (ii.2) is not satisfied, i.e., $s\varphi = \bar{\varphi}$ but there is at least one s -orbit $Q, sQ, \dots, s^{\ell-1}Q$ on $(1 + r\mathbb{Z}_{n'r})/\mu_q$ whose length ℓ is odd. Then, by Lemma 5.2, $\varphi(Q) = \frac{1}{2}p^{\nu_p(n)}$. So it has to be the case that the prime $p = 2$ and $\nu_2(n) \geq 1$; i.e., (ii.1) is satisfied.

(ii) \implies (i). First assume that the condition (ii.1) holds. We take a q -coset function $\varphi : (1 + r\mathbb{Z}_{n'r})/\mu_q \rightarrow [0, 2^{\nu_2(n)}]$ as follows:

$$\varphi(Q) = \frac{1}{2} \cdot 2^{\nu_2(n)}, \quad \forall Q \in (1 + r\mathbb{Z}_{n'r})/\mu_q. \quad (5.2)$$

Then Lemma 5.2 (iii) is satisfied obviously, so $s\varphi = \bar{\varphi}$.

Next assume that the condition (ii.2) holds. We take an integer d such that $0 \leq d < p^{\nu_p(n)}$, and define a q -coset function $\varphi : (1 + r\mathbb{Z}_{nr})/\mu_q \rightarrow [0, p^{\nu_p(n)}]$ as follows: for each s -orbit $Q, sQ, \dots, s^{\ell-1}Q$ of length ℓ on $(1 + r\mathbb{Z}_{nr})/\mu_q$, since ℓ is even, we can set

$$\varphi(s^i Q) = \begin{cases} d, & i \text{ is even;} \\ p^{\nu_p(n)} - d, & i \text{ is odd.} \end{cases} \quad (5.3)$$

Then the condition (iv.a) of Lemma 5.2 holds for all s -orbits on $(1 + r\mathbb{Z}_{nr})/\mu_q$. Thus, by Lemma 5.2, $s\varphi = \bar{\varphi}$. \square

We state some facts for the semisimple case which come from [4]. Note that a duadic λ' -constacyclic code over \mathbb{F}_q of length n' is corresponding to a partition $(1 + r\mathbb{Z}_{n'r})/\mu_q = \mathcal{X} \cup \mathcal{X}'$ and an $s \in \mathbb{Z}_{n'r}^* \cap (1 + r\mathbb{Z}_{n'r})$ such that $s\mathcal{X} = \mathcal{X}'$.

Lemma 5.5. *The following three statements are equivalent to each other:*

- (i) *There is an integer s with $\gcd(s, n'r) = 1$ and $s \equiv 1 \pmod{r}$ such that the length of any s -orbit on $(1 + r\mathbb{Z}_{n'r})/\mu_q$ is even.*
- (ii) *The duadic λ' -constacyclic codes over \mathbb{F}_q of length n' exist.*
- (iii) *q is odd and one of the following two conditions holds:*
 - (iii.1) $\nu_2(n') \geq 1$ and $\nu_2(q - 1) > \nu_2(r) \geq 1$;
 - (iii.2) $\nu_2(r) = 1$ and $\min\{\nu_2(q + 1), \nu_2(n')\} \geq 2$.

Proof. From [4, Lemma 6] we can get the equivalence of (i) and (ii). By [4, Corollary 14], (ii) is equivalent to (iii). \square

Theorem 5.6. *The isometrically p^h -self-dual λ -constacyclic codes over \mathbb{F}_q of length n exist if and only if one of the following three conditions holds:*

- (i) $p = 2$ and $\nu_2(n) \geq 1$.
- (ii) p is odd, $\nu_2(n') \geq 1$ and $\nu_2(q - 1) > \nu_2(r) \geq 1$.
- (iii) p is odd, $\nu_2(r) = 1$ and $\min\{\nu_2(q + 1), \nu_2(n')\} \geq 2$.

Proof. First we prove the necessity. Assume that $C_\varphi \leq R_{n,\lambda}$ is an isometrically p^h -self-dual λ -constacyclic code. By Lemma 5.2, there is an integer s with $\gcd(s, n'r) = 1$ and $s \equiv 1 \pmod{r}$ such that $s\varphi = \bar{\varphi}$. By Lemma 5.4, either (i) of the theorem holds, or the length of any s -orbit on $(1 + r\mathbb{Z}_{n'r})/\mu_q$ is even, hence, by Lemma 5.5 (iii), one of the (ii) and (iii) of the theorem holds.

Next we prove the sufficiency. If one of the conditions (ii) and (iii) holds, then, by Lemma 5.5, there is an integer s with $\gcd(s, n'r) = 1$ and $s \equiv 1 \pmod{r}$ such that the length of any s -orbit on $(1 + r\mathbb{Z}_{n'r})/\mu_q$ is even. Thus, the sufficiency is deduced from Lemma 5.4 and Lemma 5.2 at once. \square

Corollary 5.7. *The following three statements are equivalent:*

- (i) *There is an $h \in [0, e]$ such that the isometrically p^h -self-dual λ -constacyclic codes of length n over \mathbb{F}_q exist.*
- (ii) *For any $h \in [0, e]$, the isometrically p^h -self-dual λ -constacyclic codes of length n over \mathbb{F}_q exist.*
- (iii) *either $p = 2$ and $\nu_2(n) \geq 1$, or the duadic λ' -constacyclic codes over \mathbb{F}_q of length n' exist.*

Proof. The necessary and sufficient condition for the existence of isometrically p^h -self-dual constacyclic codes stated in Theorem 5.6 is independent of the choice of $h \in [0, e]$; hence the equivalence of (i) and (ii) is obtained. And, by Lemma 5.5, the statement (iii) is equivalent to the existence condition stated in Theorem 5.6. \square

6 Galois self-dual constacyclic codes

In this section we show a necessary and sufficient condition for the existence of Galois self-dual constacyclic codes. We begin with a characterization of the Galois self-dual constacyclic codes by q -coset functions.

Theorem 6.1. *Let $h \in [0, e]$, and $\varphi : (1 + r\mathbb{Z}_{n'r})/\mu_q \rightarrow [0, p^{\nu_p(n)}]$ be a q -coset function. Then the following two statements are equivalent to each other.*

- (i) $C_\varphi = C_\varphi^{\perp h}$ (i.e., C_φ is p^h -self-dual).
- (ii) $r \mid \gcd(p^h + 1, p^e - 1)$ (i.e., $-p^h$ and $p^e \equiv 1 \pmod{r}$) and $-p^h\varphi = \bar{\varphi}$.

Proof. By Theorem 4.4, $C_\varphi^{\perp h} = C_{-p^{e-h}\bar{\varphi}}$ which is a $\lambda^{-p^{e-h}}$ -constacyclic code. We get that $C_\varphi = C_\varphi^{\perp h}$ if and only if $\lambda^{-p^{e-h}} = \lambda$ and $C_\varphi = C_{-p^{e-h}\bar{\varphi}}$. That is, $C_\varphi = C_\varphi^{\perp h}$ if and only if $-p^{e-h} \equiv 1 \pmod{r}$ and $\varphi = -p^{e-h}\bar{\varphi}$. Since $r \mid (q - 1)$ where $q = p^e$, we have $p^e \equiv 1 \pmod{r}$. Hence

$$(-p^h)(-p^{e-h}) = p^e \equiv 1 \pmod{r}.$$

We see that $-p^{e-h} \equiv 1 \pmod{r}$ if and only if $-p^h \equiv 1 \pmod{r}$. Multiplying $-p^h$ to the both sides of the equality $\varphi = -p^{e-h}\bar{\varphi}$, we get $-p^h\varphi = (-p^h)(-p^{e-h})\bar{\varphi}$. However, by Corollary 3.8, $(-p^h)(-p^{e-h})\bar{\varphi} = \bar{\varphi}$. In conclusion, $C_\varphi = C_\varphi^{\perp h}$ if and only if $-p^h \equiv 1 \pmod{r}$ and $-p^h\varphi = \bar{\varphi}$. \square

We need a number-theoretic result.

Lemma 6.2. *Let k be an odd integer, and d be a positive integer.*

- (i) *If $k = 1 + 2^v u$ with $v \geq 2$ and $2 \nmid u$ (equivalently, $k \equiv 1 \pmod{4}$), then*

$$\nu_2(k^d - 1) = v + \nu_2(d), \quad \nu_2(k^d + 1) = 1.$$

- (ii) *If $k = -1 + 2^v u$ with $v \geq 2$ and $2 \nmid u$ (equivalently, $k \equiv -1 \pmod{4}$), then*

- (ii.1) *if $\nu_2(d) = 0$ (i.e., d is odd) then*

$$\nu_2(k^d - 1) = 1, \quad \nu_2(k^d + 1) = v;$$

- (ii.2) *if $\nu_2(d) \geq 1$ (i.e., d is even) then*

$$\nu_2(k^d - 1) = v + \nu_2(d), \quad \nu_2(k^d + 1) = 1.$$

Proof. (i). If d is a prime integer; by the Newton's binomial formula it is easy to check that

$$k^d = \begin{cases} 1 + 2^{v+1}u', & d = 2; \\ 1 + 2^v u', & d \neq 2; \end{cases} \quad \text{with } 2 \nmid u'.$$

For any positive integer d , decomposing d into a product of primes, we can get

$$k^d = 1 + 2^{v+\nu_2(d)}u', \quad \text{with } 2 \nmid u'.$$

Then it is obvious that $\nu_2(k^d - 1) = v + \nu_2(d)$ and $\nu_2(k^d + 1) = 1$.

(ii). Similarly to the above, if d is a prime integer then

$$k^d = \begin{cases} 1 + 2^{v+1}u', & d = 2; \\ -1 + 2^v u', & d \neq 2; \end{cases} \quad \text{with } 2 \nmid u'.$$

For any positive integer d , similarly to the above argument again,

$$k^d = \begin{cases} 1 + 2^{v+\nu_2(d)}u', & \nu_2(d) \geq 1; \\ -1 + 2^v u', & \nu_2(d) = 0; \end{cases} \quad \text{with } 2 \nmid u'.$$

Then both (ii.1) and (ii.2) are easily derived. \square

We return to our notations on constacyclic codes.

Lemma 6.3. *Assume that $-p^h \equiv 1 \pmod{r}$. The length of any $(-p^h)$ -orbit on $(1 + r\mathbb{Z}_{n'r})/\mu_q$ is even if and only if both n' and r are even (hence p is odd) and one of the following three conditions holds:*

- (i) $p = 1 + 2^v u$ with $v \geq 2$ and $2 \nmid u$ (equivalently, $p \equiv 1 \pmod{4}$).
- (ii) $p = -1 + 2^v u$ with $v \geq 2$ and $2 \nmid u$ (equivalently, $p \equiv -1 \pmod{4}$), both e and h are even.
- (iii) $p = -1 + 2^v u$ with $v \geq 2$ and $2 \nmid u$ (equivalently, $p \equiv -1 \pmod{4}$), at least one of e and h is odd, and $\nu_2(n'r) > v$.

Proof. Note that $q = p^e$. By [4, Lemma 6], the length of any $(-p^h)$ -orbits on $(1 + r\mathbb{Z}_{n'r})/\mu_q$ is even if and only if the duadic λ -constacyclic codes over \mathbb{F}_{p^e} of length n' given by the multiplier μ_{-p^h} exist. Further, by [4, Corollary 19], the latter statement holds if and only if both n' and r are even (hence $q = p^e$ is odd) and one of the following four conditions holds (we adopt a convention that $\nu_2(0) = -\infty$ hence $|\nu_2(0)| = \infty$):

- (c1) $\nu_2(p^e - 1) > \nu_2(-p^h - 1)$ and $\nu_2(n'r) > \nu_2(-p^h - 1)$;
- (c2) $\nu_2(p^e - 1) = 1$, $\nu_2(-p^h - 1) > 1$, $\nu_2(p^e + 1) + 1 > \nu_2(-p^h - 1)$ and $\nu_2(n'r) > \nu_2(-p^h - 1)$;

- (c3) $\nu_2(p^e - 1) = \nu_2(-p^h - 1) = 1$, $|\nu_2(-p^h + 1)| > \nu_2(p^e + 1)$ and $\nu_2(n'r) > \nu_2(p^e + 1)$;
(c4) $\nu_2(p^e - 1) = \nu_2(-p^h - 1) = 1$, $|\nu_2(-p^h + 1)| < \nu_2(p^e + 1)$ and $|\nu_2(-p^h + 1)| < \nu_2(n'r)$.

It remains to show that one of the four conditions holds if and only if one of (i), (ii) and (iii) of the lemma holds. We discuss it in two cases.

Case 1: $p = 1 + 2^v u$ with $v \geq 2$ and $2 \nmid u$. At this case the condition (i) of the lemma holds. On the other hand, by Lemma 6.2,

$$\nu_2(p^e - 1) = v + \nu_2(e) \quad \text{and} \quad \nu_2(-p^h - 1) = \nu_2(p^h + 1) = 1.$$

Note that $\nu_2(n'r) \geq 2$ (since both n' and r are even), the condition (c1) holds.

Case 2: $p = -1 + 2^v u$ with $v \geq 2$ and $2 \nmid u$. There are four subcases.

Subcase 2.1: both e and h are even. By Lemma 6.2,

$$\nu_2(p^e - 1) = v + \nu_2(e), \quad \text{and} \quad \nu_2(-p^h - 1) = \nu_2(p^h + 1) = 1.$$

The condition (c1) holds, and the condition (ii) of the lemma holds.

Subcase 2.2: e is even, h is odd. As we have seen, $\nu_2(p^e - 1) = v + \nu_2(e)$. None of (c2), (c3) and (c4) holds. Further, since h is odd, by Lemma 6.2, $\nu_2(-p^h - 1) = \nu_2(p^h + 1) = v$. So, (c1) holds if and only if $\nu_2(n'r) > \nu_2(-p^h - 1) = v$; and if it is, (iii) of the lemma also holds.

Subcase 2.3: e is odd, h is even. Then $\nu_2(p^e - 1) = 1$ so that (c1) cannot hold. And, since $\nu_2(-p^h - 1) = \nu_2(p^h + 1) = 1$, (c2) does not hold. Further,

$$\nu_2(-p^h + 1) = \nu_2(p^h - 1) = v + \nu_2(h) > v = \nu_2(p^e + 1),$$

which implies that (c4) is not satisfied. The condition (c3) is satisfied provided $\nu_2(n'r) > \nu_2(p^e + 1) = v$, which is also required by (iii) of the lemma.

Subcase 2.4: e is odd, and h is odd. Then

$$\nu_2(p^e - 1) = 1, \quad \nu_2(p^e + 1) = v, \quad \nu_2(p^h + 1) = v, \quad \nu_2(p^h - 1) = 1.$$

None of the conditions (c1), (c3) and (c4) holds. Note that one more requirement " $\nu_2(n'r) > \nu_2(p^h + 1) = v$ " makes (c2) held, and it also makes (iii) of the lemma held. \square

Theorem 6.4. *The p^h -self-dual λ -constacyclic codes over \mathbb{F}_q of length n exist if and only if $r \mid \gcd(p^h + 1, p^e - 1)$ and one of the following holds:*

- (i) $p = 2$ and $\nu_2(n) \geq 1$.
- (ii) $p = 1 + 2^v u$ with $v \geq 2$ and $2 \nmid u$ (equivalently, $p \equiv 1 \pmod{4}$), both n' and r are even.

- (iii) $p = -1 + 2^v u$ with $v \geq 2$ and $2 \nmid u$ (equivalently, $p \equiv -1 \pmod{4}$), all of n', r, e and h are even.
- (iv) $p = -1 + 2^v u$ with $v \geq 2$ and $2 \nmid u$ (equivalently, $p \equiv -1 \pmod{4}$), both n' and r are even, but at least one of e and h is odd, and $\nu_2(n'r) > v$.

Proof. By Theorem 6.1, the p^h -self-dual λ -constacyclic codes over \mathbb{F}_q of length n exist if and only if $r \mid (p^h + 1)$ and there is a q -coset function $\varphi : (1 + r\mathbb{Z}_{n'r})/\mu_q \rightarrow [0, p^{\nu_p(n)}]$ such that $-p^h \varphi = \bar{\varphi}$. By Lemma 5.4, $-p^h \varphi = \bar{\varphi}$ if and only if either (i) of the theorem holds or the length of any $(-p^h)$ -orbit on $(1 + r\mathbb{Z}_{n'r})/\mu_q$ is even. Further, the length of any $(-p^h)$ -orbit on $(1 + r\mathbb{Z}_{n'r})/\mu_q$ is even if and only if one of the conditions (i), (ii) and (iii) in Lemma 6.3 holds, they are restated in the theorem relabeled by (ii), (iii) and (iv). \square

Corollary 6.5. *Self-dual λ -constacyclic codes over \mathbb{F}_q of length n exist if and only if one of the following holds:*

- (i) $p = 2$, $\lambda = 1$ and $\nu_2(n) \geq 1$.
- (ii) $p^e \equiv 1 \pmod{4}$, $\lambda = -1$, n' is even.
- (iii) $p^e \equiv -1 \pmod{4}$, $\lambda = -1$, and $\nu_2(n') + 1 > \nu_2(p^e + 1)$.

Proof. Take $h = 0$ in Theorem 6.4. The condition that $r \mid \gcd(p^h + 1, p^e - 1)$ implies that $r \mid 2$. Then Theorem 6.4 (i) is reduced to $p = 2$, $\nu_2(n) \geq 1$, hence $r = 1$. And Theorem 6.4 (ii) and (iii) are reduced to $p^e \equiv 1 \pmod{4}$, $r = 2$ and n' is even. Finally, Theorem 6.4 (iv) is reduced to $p^e \equiv -1 \pmod{4}$, $r = 2$ and $\nu_2(n') + 1 > \nu_2(p^e + 1)$. \square

We remark that (i) of Corollary 6.5 is the cyclic (but not semisimple) case. In [23] there is a similar result for any group codes. On the other hand, if it is restricted to the semisimple case, then Corollary 6.5 (i) is not allowed, and $n' = n$ (recall that $n = p^{\nu_p(n)} n'$). So [1, Theorem 3] or [4, Corollary 21] are obtained as a consequence of Corollary 6.5.

Corollary 6.6. *Hermitian self-dual λ -constacyclic codes over \mathbb{F}_q of length n exist if and only if e is even, $r \mid \gcd(p^{\frac{e}{2}} + 1, p^e - 1)$ and one of the following holds:*

- (i) $p = 2$ and $\nu_2(n) \geq 1$.
- (ii) $p^{\frac{e}{2}} \equiv 1 \pmod{4}$, both n' and r are even.
- (iii) $p^{\frac{e}{2}} \equiv -1 \pmod{4}$, both n' and r are even, $\nu_2(n'r) > \nu_2(p^{\frac{e}{2}} + 1)$.

Proof. In Theorem 6.4, let e be even and $h = \frac{e}{2}$. So $r \mid \gcd(p^{\frac{e}{2}} + 1, p^e - 1)$. Then (i) of the corollary is just the (i) of Theorem 6.4. By Lemma 6.2, Theorem 6.4 (ii) and (iii) are reduced to the (ii) of the corollary. Finally, when $p = -1 + 2^v u$ with $v \geq 2$ and $2 \nmid u$, $\frac{e}{2}$ is odd if and only if $p^{\frac{e}{2}} \equiv -1 \pmod{4}$; and at that case, $v = \nu_2(p^{\frac{e}{2}} + 1)$; see Lemma 6.2. So Theorem 6.4 (iv) is reduced to (iii) of the corollary. \square

7 Examples

The first example is constructed in the way of Eqn (5.2) to illustrates the repeated-root case where $p = 2$.

Example 7.1. Let $p = 2$, $e = 2$, i.e., $q = 4$, and let $\theta \in \mathbb{F}_4$ be a primitive third root of unity, i.e., $\mathbb{F}_4 = \{0, 1, \theta, \theta^2\}$ and $\theta^2 + \theta + 1 = 0$. Let $n = 2$, hence $\nu_2(n) = 1$ and $n' = 1$.

(i) Take $\lambda = \theta^2$ (so $r = 3$). Then $r \mid \gcd(2^1 + 1, 2^2 - 1)$ and Corollary 6.6 (i) holds, so an Hermitian self-dual θ^2 -constacyclic code exists (but the self-dual θ^2 -constacyclic codes do not exist). In fact, $X^2 - \theta^2 = (X - \theta)^2$, and $1 + r\mathbb{Z}_{n'r} = \{1\}$. The q -coset function $\varphi(1) = 1$ (then $\bar{\varphi} = \varphi$) is corresponding to the θ^2 -constacyclic code $C_\varphi \leq R_{2,\theta^2}$ generated by $X + \theta$, i.e.,

$$C_\varphi = \langle X + \theta \rangle = \{(0, 0), (\theta, 1), (\theta^2, \theta), (1, \theta^2)\},$$

which is Hermitian self-dual since $-3\varphi = \bar{\varphi}$. Also, a direct computation is as follows:

$$\langle (\theta, 1), (\theta, 1) \rangle_1 = \theta \cdot \theta^2 + 1 \cdot 1^2 = 1 + 1 = 0.$$

(ii) However, if take $\lambda = 1$ (i.e., $r = 1$), then a self-dual cyclic code exists (which is also an Hermitian self-dual cyclic code) as follows: $X^2 + 1 = (X + 1)^2$, $1 + r\mathbb{Z}_{n'r} = \{1\}$, take q -coset function $\psi(1) = 1$, then $C_\psi \leq R_{2,1}$ is a self-dual cyclic code.

The next example is also the repeated-root case, but it is constructed in the way of Eqn (5.3).

Example 7.2. Let $p = 3$, $e = 4$ hence $q = 3^4$. Then \mathbb{F}_q contains a primitive 16-th root of unity. Take $\lambda = \theta^{12}$ and $n = 3 \cdot 4$. Hence $r = 4$, $\lambda' = \theta^4$, $\nu_3(n) = 1$, $n' = 4$, $[0, 3^{\nu_3(n)}] = \{0, 1, 2, 3\}$, $1 + r\mathbb{Z}_{n'r} = \{1, 5, 9, 13\}$ whose elements are all fixed by $\mu_q = \mu_{3^4}$, and

$$X^{12} - \lambda = (X^4 - \theta^4)^3 = (X - \theta)^3(X - \theta^5)^3(X - \theta^9)^3(X - \theta^{13})^3.$$

Define a q -coset function $\varphi : 1 + r\mathbb{Z}_{n'r} \rightarrow [0, 3]$ by

$$\varphi(1) = 1, \quad \varphi(5) = 2, \quad \varphi(9) = 1, \quad \varphi(13) = 2.$$

Then

$$f_\varphi(X) = (X - \theta)(X - \theta^5)^2(X - \theta^9)(X - \theta^{13})^2.$$

We can consider the θ^{12} -constacyclic code $C_\varphi \leq R_{12,\theta^{12}}$ with check polynomial $f_\varphi(X)$. It is easy to check that $-3\varphi = \bar{\varphi}$. We have the following conclusions.

- By Theorem 6.1, C_φ is a 3^1 -self-dual θ^{12} -constacyclic code.
- By Corollary 6.5 and Corollary 6.6, C_φ is neither self-dual nor Hermitian self-dual, because $r \neq 2$ and $r \nmid \gcd(3^2 + 1, 3^4 - 1)$.

- By Lemma 5.2, for any $h \in [0, 4]$, the C_φ is an isometrically 3^h -self-dual θ^{12} -constacyclic codes of length 12 over \mathbb{F}_{3^4} . For example, because (cf. Lemma 5.2)

$$\mathcal{M}_{(-3^{\frac{4}{2}})(-3)}(C_\varphi) = \mathcal{M}_{-3^{\frac{4}{2}}}(C_{-3\varphi}) = \mathcal{M}_{-3^{\frac{4}{2}}}(C_{\bar{\varphi}}) = C_\varphi^{\perp^{\frac{4}{2}}},$$

the code C_φ is isometrically Hermitian self-dual.

The following example shows that a constacyclic code can be both self-dual and Hermitian self-dual.

Example 7.3. Let $p = 3$, $q = 9$ (i.e., $e = 2$), $\lambda = -1$ (i.e., $r = 2$) and $n = 4$. Then $\nu_p(n) = \nu_3(4) = 0$ (i.e., it is the semisimple case: $n = n' = 4$), $n'r = 4 \cdot 2 = 8$, $1 + r\mathbb{Z}_{n'r} = \{1, 3, 5, 7\}$ on which $\mu_q = \mu_9$ is the identity permutation. Take a q -coset function φ as follows:

$$\varphi(1) = \varphi(3) = 0, \quad \varphi(5) = \varphi(7) = 1.$$

Then

$$\bar{\varphi}(1) = \bar{\varphi}(3) = 1, \quad \bar{\varphi}(5) = \bar{\varphi}(7) = 0.$$

It is easy to check that

$$\varphi = -\bar{\varphi}, \quad \varphi = -3\bar{\varphi}$$

Thus, $C_\varphi \leq R_{4,-1}$ is a $[4, 2, 3]$ negacyclic code over \mathbb{F}_9 which is both self-dual and Hermitian self-dual.

In many cases the self-dual constacyclic codes and Hermitian self-dual constacyclic codes both exist, but there is no constacyclic code which is both self-dual and Hermitian self-dual.

Example 7.4. Let $p = 5$, $e = 2$, i.e., $q = 5^2 = 25$. Take $r = 2$ (i.e., $\lambda = -1$), $n = 26$. Then $n' = n = 26$ (i.e., $\nu_p(n) = 0$), $n'r = 52$, $X^{26} + 1$ has no multiple roots and $\mathbb{F}_{25}[X]/\langle X^{26} + 1 \rangle$ is semisimple. Consider

$$1 + r\mathbb{Z}_{n'r} = 1 + 2\mathbb{Z}_{52} = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, \\ 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51\}.$$

The q -cosets are (where $Q_i = \{i, iq, iq^2, \dots\}$ denotes the q -coset containing i):

$$(1 + r\mathbb{Z}_{n'r})/\mu_q = (1 + 2\mathbb{Z}_{52})/\mu_{25} = \{ Q_1, Q_3, Q_5, Q_7, Q_9, Q_{11}, Q_{13}, \\ Q_{27}, Q_{29}, Q_{31}, Q_{33}, Q_{35}, Q_{37}, Q_{39} \}.$$

where

$$\begin{aligned} Q_1 &= \{1, 25\}, & Q_3 &= \{3, 23\}, & Q_5 &= \{5, 21\}, \\ Q_7 &= \{7, 19\}, & Q_9 &= \{9, 17\}, & Q_{11} &= \{11, 15\}, & Q_{13} &= \{13\}, \\ Q_{27} &= \{27, 51\}, & Q_{29} &= \{29, 49\}, & Q_{31} &= \{31, 47\}, \\ Q_{33} &= \{33, 45\}, & Q_{35} &= \{35, 43\}, & Q_{37} &= \{37, 41\}, & Q_{39} &= \{39\} \end{aligned}$$

The orbits of μ_{-1} on $(1 + 2\mathbb{Z}_{52})/\mu_{25}$ are as follows:

$$\{Q_1, Q_{27}\}, \{Q_3, Q_{29}\}, \{Q_5, Q_{31}\}, \{Q_7, Q_{33}\}, \{Q_9, Q_{35}\}, \{Q_{11}, Q_{37}\}, \{Q_{13}, Q_{39}\}.$$

The orbits of μ_{-5} on $(1 + 2\mathbb{Z}_{52})/\mu_{25}$ are as follows:

$$\{Q_1, Q_{31}\}, \{Q_3, Q_{37}\}, \{Q_5, Q_{27}\}, \{Q_7, Q_9\}, \{Q_{11}, Q_{29}\}, \{Q_{33}, Q_{35}\}, \{Q_{13}, Q_{39}\}.$$

Correspondingly, we define two q -coset functions φ_{-1} , φ_{-5} as follows:

$$\varphi_{-1}(Q_j) = \begin{cases} 0, & j = 1, 3, 5, 7, 9, 11, 13; \\ 1, & j = 27, 29, 31, 33, 35, 37, 39. \end{cases}$$

$$\varphi_{-5}(Q_j) = \begin{cases} 0, & j = 1, 3, 5, 7, 11, 13, 33; \\ 1, & j = 9, 27, 29, 31, 35, 37, 39. \end{cases}$$

Then the negacyclic code $C_{\varphi_{-1}} \leq R_{26,-1}$ over \mathbb{F}_{25} is 5^0 -self-dual (i.e., self-dual), but not 5^1 -self-dual (i.e., not Hermitian self-dual). On the other hand, the negacyclic code $C_{\varphi_{-5}} \leq R_{26,-1}$ over \mathbb{F}_{25} is 5^1 -self-dual (i.e., Hermitian self-dual), but not 5^0 -self-dual (i.e., not self-dual).

Acknowledgements

The research of the authors is supported by NSFC with grant number 11271005.

References

- [1] T. Blackford, Negacyclic duadic codes, *Finite Fields Appl.*, **14**(2008), 930-943.
- [2] T. Blackford, Isodual constacyclic codes, *Finite Fields Appl.*, **24**(2013), 29-44.
- [3] R. A. Brualdi, V. Pless, Polyadic codes, *Discr. Appl. Math.*, **25**(1989), 3-17.
- [4] Bocong Chen, H. Q. Dinh, Yun Fan, San Ling, Polyadic constacyclic codes, *IEEE Trans. Inform. Theory* **61**(2015), no.9, 4895-4904.
- [5] Bocong Chen, Yun Fan, Liren Lin, Hongwei Liu, Constacyclic codes over finite fields, *Finite Fields Appl.*, **18**(2012), 1217-1231.
- [6] H. Q. Dinh, Repeated-root constacyclic codes of length $2ps$, *Finite Fields Appl.* **18** (2012) 133-143.
- [7] H. Q. Dinh, Lopez-Permouth, Cyclic and negacyclic codes over finite chain rings, *IEEE Trans. Inform. Theory* **50**(2004), no.8, 1728-1744.

- [8] C. Ding, V. Pless, Cyclotomy and duadic codes of prime lengths, *IEEE Trans. Inform. Theory*, **45**(1999), 453-466.
- [9] C. Ding, K.Y. Lam, C. Xing, Enumeration and construction of all duadic codes of length p^m , *Fund. Inform.* **38**(1999), 149-161.
- [10] Yun Fan, Guanghui Zhang, On the existence of self-dual permutation codes of finite groups, *Des. Codes Cryptogr.*, **62**(2012), 19-29.
- [11] Yun Fan, Liang Zhang, Iso-orthogonality and Type-II duadic constacyclic codes, *arXiv:1501.01352*, 2015.
- [12] S. Han, J-L. Kim, Computational results of duadic double circulant codes, *J. Appl. Math. Comput.*, **40**(2012), 33-43.
- [13] W.C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.
- [14] S. Jitman, S. Ling, P. Solé, Hermitian self-dual Abelian codes, *IEEE Trans. Inform. Theory*, **60**(2014), 1496-1507.
- [15] J. S. Leon, J. M. Masley, V. Pless, Duadic codes, *IEEE Trans. Inform. Theory*, **30**(1984), 709-714.
- [16] C. J. Lim, Consta-abelian polyadic codes, *IEEE Trans. Inform. Theory*, **51**(2005), no. 6, 2198-2206.
- [17] S. Ling, C. Xing, Polyadic codes revisited, *IEEE Trans. Inform. Theory*, **50**(2004), 200-207.
- [18] C. Martinez-Pérez, W. Willems, Self-dual codes and modules for finite groups in characteristic two, *IEEE Trans. Inform. Theory* **50**(2004), no. 8, 1798-1803.
- [19] V. Pless, Duadic codes revisited, *Congressus Numeratium*, **59**(1987), 225-233.
- [20] J. J. Rushanan, Duadic codes and difference sets, *J. Combin. Theory Set. A*, **57**(1991), 254-61.
- [21] M. H. M. Smid, Duadic codes, *IEEE Trans. Inform. Theory*, **33**(1987), 432-433.
- [22] A. Sharma, G.K. Bakshi, V.C. Dumir, M. Raka, Cyclotomic numbers and primitive idempotents in the ring $GF(q)[X]/(x^{p^n} - 1)$, *Finite Fields Appl.* **10** (4) (2004) 653-673.
- [23] W. Willems, A note on self-dual group codes, *IEEE Trans. Inform. Theory* **48**(2002), 3107-3109.
- [24] H. N. Ward, L. Zhu, Existence of abelian group codes partitions, *J. Combin. Theory Ser. A*, **67**(1994), 276-281.